Continuation of Application for Search Warrant

Based on my knowledge, training and experience, I, Benjamin Glynn, being duly sworn, depose and state as follows:

INTRODUCTION

1. Based on the information set forth below, there is probable cause to believe that evidence of violations of federal law, specifically, conspiracy to commit wire fraud in violation of 18 U.S.C. §§ 1343 and 1349, access device fraud in violation of 18 U.S.C. § 1029(a)(2), and aggravated identify theft in violation of 18 U.S.C. § 1028(a)(1), will be found on a certain cellular phone(hereinafter the "**Subject Device**," described more fully in Attachment A). The categories of electronically stored information and evidence sought are described in Attachment B.

2. The **Subject Device** was seized on May 17, 2018, pursuant to the execution of search warrant 218-MJ-1201 on a 2005 Honda Odyssey which was located near 1334 Jeffrey Way in San Bernardino, California. The vehicle belonged to and was driven by Ion ZAMFIR, who was indicted on May 8, 2018 for his involvement in an Automated Teller Machine (ATM) Skimming ring which was active in the Western District of Michigan in late 2017 and early 2018. The warrant authorized the seizure of the **Subject Device**, and it is currently in the custody of law enforcement. This Application seeks the issuance of a warrant to examine the **Subject Device**.

APPLICANT'S TRAINING AND EXPERIENCE

3. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been so employed for over 1 year. Prior to being hired by the FBI I was a police officer/investigator for the Rock Hill Police Department in Rock Hill, SC for six years. During my time as an Agent and investigator, I have been involved in numerous investigations which involved the exploitation of cellular telephone data in furtherance of said investigations. I am currently assigned to the St Joseph Resident Agency of the Detroit Field Office. I have participated in numerous search warrants, interviews, investigations, and training involving federal crimes.

4. I know from my training and experience that those involved in ATM skimming frequently utilize mobile telephones to communicate with their co-conspirators and facilitate ATM skimming. Mobile phones often contain evidence indicative of ATM skimming, including records of incoming and outgoing calls and text messages with co-conspirators; voicemail messages; photographs of ATM's and skimming devices, co-conspirators, or currency; and, in the case of "smart phones," Global Positioning System (GPS) data indicating the location of the device at given points in time, providing evidence that the device was in the area where the ATM skimming occurred. Further, these types of devices are frequently used to access social media websites such as Facebook, Instagram, etc. In my training and experience, ATM skimmers are using social media with increasing frequency to communicate with co-conspirators.

PROBABLE CAUSE

5. In late 2017 and early 2018, IONEL SYDNEY MIHAI, ION ZAMFIR, a/k/a Noris Nor, and others conspired to fraudulently obtain cash from Automated Teller Machines ("ATMs") in the Western District of Michigan and elsewhere. In this conspiracy, the conspirators placed thin electronic devices inside of the financial card slot of ATMs which were capable of capturing the data from the data strip of financial transaction cards used by customers after the device placement. Additionally, a pin-hole camera was also placed to observe the pin number entered by the customer. After a brief period of time, typically between 12 and 24 hours, the skimming devices were removed and the data gleaned was placed onto new, fraudulent financial transaction cards. These new cards were used by the suspects to then fraudulently remove money from the customer/victim accounts. This type of fraud is commonly referred to as a "skimming attack."

6. In order to avoid detection, the conspirators bought and sold vehicles frequently. They often used the internet to conduct these transactions. For example, the conspirators used the website Offerup.com, which is similar to Craigslist, to buy and sell cars.

7. On numerous dates in December of 2017 and January and February of 2018, MIHAI and ZAMFIR were captured on video by surveillance cameras mounted on Automated Teller Machines in West Michigan and elsewhere removing skimming devices and conducting subsequent fraudulent cash withdrawals.

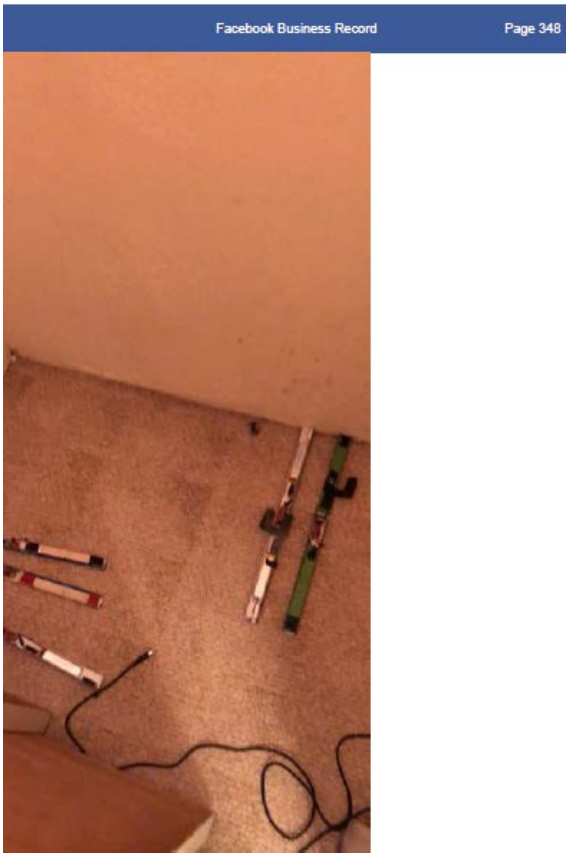
8. MIHAI was indicted by a Grand Jury in the Western District of Michigan on April 12, 2018, in connection with the skimming attacks. He was charged with conspiring to commit wire fraud, in violation of 18 U.S.C. 1349 and 1343, access device fraud, in violation of 18 U.S.C. 1029, and aggravated identity theft in violation of 18 U.S.C. 1028A.

9. ZAMFIR was indicted by a Grand Jury in the Western District of Michigan on May 8, 2018, in a Superseding Indictment charging him and MIHAI with conspiring to commit wire fraud, in violation of 18 U.S.C. §§ 1349 and 1343, access device fraud, in violation of 18 U.S.C. § 1029, and aggravated identity theft in violation of 18 U.S.C. § 1028A. The Superseding Indictment alleges that ZAMFIR, MIHAI, and other conspirators committed the crimes between October 2017 and March 2018.

10. As part of the investigation of the case, agents viewed publicly available Facebook posts of conspirators, and also obtained search warrants for the contents of some of the conspirators' Facebook accounts. A review of these Facebook accounts revealed that the conspirators took pictures of themselves, apparently with cellphones, and often posted them on Facebook. Some of these photos are of evidentiary value. For example, agents reviewing Facebook accounts observed a post from December 31, 2017 in which an individual who is a visual match to ZAMFIR, a/k/a Noris Nor, standing next to a white Range Rover near a Hampton Inn hotel. This picture appears to have been taken with a cellular phone:

11. The white Range Rover appears to by a visual match to a white Range Rover that was used by Ionel MIHAI and ZAMFIR on December 31, 2017 to commit ATM skimming at a United Federal Credit Union (UFCU) in Holland, MI. An the Ottawa County Sheriff's Detective was provided a screen shot image of the Facebook post and identified the exact location in Holland, MI where it was taken.

12. On another occasion, the conspirators posted on social media a picture of what appears to be skimming devices that are used to conduct the skimming attacks against ATMs. Again, this picture appears to have been taken with a cellphone:



13. Additionally, there was a photograph of ZAMFIR with a large quantity of money which was sent by ZAMFIR on social media on January 9, 2018. This is significant because during January 6-8, 2018, ZAMFIR and others were highly active conducting fraudulent cash withdrawals in the Grand Rapids, MI and Chicago, IL areas with the data gleaned from prior skimming attacks in the Southwestern Michigan area:

14. Due to the prevalent use of cell phones to take photographs and "selfies" such as these, it is likely that ZAMFIR took these photographs using the **Subject Device.**

15. As set forth above, ZAMFIR was indicted by a Grand Jury in the Western District of Michigan on May 8, 2018. A federal arrest warrant was issued based on the indictment and ZAMFIR was located and arrested on May 17, 2018 in San Bernardino, CA. When ZAMFIR was arrested in May 2018, he was travelling to California from Colorado with a group of individuals who were travelling two in two vehicles. A search of one of the passengers of the vehicle in which ZAMFIR was not travelling revealed that she had $62,600 in cash hidden under her dress, suggesting that ZAMFIR and the other individuals had engaged in further skimming attacks.

16. A search warrant for ZAMFIR's 2005 Honda Odyssey was issued in the Central District of California. Pursuant to the search warrant, investigators seized the **Subject Device**, a black Apple iPhone X, no serial number attainable from outside the device. The **Subject Device** was recovered during the search of ZAMFIR's 2005 Honda Odyssey, for which investigators had both verbal consent and a federal search warrant to search. The **Subject Device** was located in the center console area and both ZAMFIR and IANCU acknowledged it was ZAMFIR's phone.

17. The **Subject Device** is currently in storage at the FBI St Joseph Resident Office. The **Subject Device** has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the **Subject Device** was first seized on May 17, 2018.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

18. Based on my training and experience, the Subject Device is a wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

19. Based on my training, experience, and research I know that the **Subject Device** has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device. Users of the **Subject Device** can send text messages, pictures, and other media, and can access the internet and social media with it. In my training and experience, examining data

stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

20. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

21. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper

context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when.

22. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

23. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I

submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

24. I respectfully submit that there is probable cause to believe that Ion ZAMFIR, Ionel MIHAI, and coconspirators of the ATM skimming scheme have conspired to commit wire fraud, access device fraud, and aggravated identify theft in violation of 18 U.S.C. §§ 1343 and 1349, 18 U.S.C. § 1029(a)(2), and 18 U.S.C. § 1028(a)(1). I submit that this application supplies probable cause for a search warrant authorizing the examination of the **Subject Device** described in Attachment A to seek the items described in Attachment B.